

Patent Claims

1. Procedure for the increased security of authentication processes in digital mobile radio systems is characterized by several different secret SIM-specific codes (KI) that are stored in the mobile radio network and in the subscriber identification module (SIM), and one code (KI) that is selected for the execution of the authentication between subscriber identification module and the mobile radio network of the SIM from several stored secret codes.
2. Procedure, according to claim 1, is characterized by the selection of the code (KI) by the subscriber identification module (SIM), according to the random principle.
3. Procedure, according to claims 1 or 2, is characterized by the mobile radio network that, with special algorithms under specification of a random number (RAND) determines a SRES/KC-pair for all SIM-specific codes (KI) forming, with the respective RAND, RAND/SRES/KC-triplets.
4. Procedure, according to one of the claims 1 to 3, is characterized by the formed RAND/SRES/KC-triplets that are stored in the mobile radio network.
5. Procedure, according to one of the claims 1 to 4, is characterized by a RAND of one of these triplets, that is sent to the subscriber identification module from the mobile radio network to initiate the authentication.

007564-0544

sub-91

6. Procedure, according to one of the claims 1 to 5, is characterized by the subscriber identification module that calculates the corresponding values for SRES and KC by the transmitted RAND and the selected code (KI), and sends the determined answer to the mobile radio network.
7. Procedure, according to one of the claims 1 to 6, is characterized by the comparison made to verify agreement or conformity of the received SRES with all of the stored SRES for the utilized RAND in the mobile radio network.
8. Procedure, according to one of the claims 1 to 7, is characterized by the mobile radio network and the SIM, which is used to encode the transfer or transmission of the matching SRES corresponding KC.

sub-
cont

00706464-052404